Partly Cloudy IPA

Joining Cloud VMs to FreeIPA

André Boscatto

Sr. Product Owner for Identity and Access Management in RHEL

SSSD | Samba | IdM Insights

What we'll discuss today

- **The problem**: pain-free identity management in hybrid cloud envs
- **Solution overview**: the Podengo project
- Brief **technical details**
- **Demo** time!
- **Gaps**, future directions, **opportunities**

Introductions

- I work in the Identity Management team at Red Hat
- The Podengo project is the hard work of a small sub-team, assisted by many collaborators (service delivery, UX, docs, …)
- This presentation is also a collaboration (already presented at *Everything Open 2025* and to be presented at *DevConf.in*)

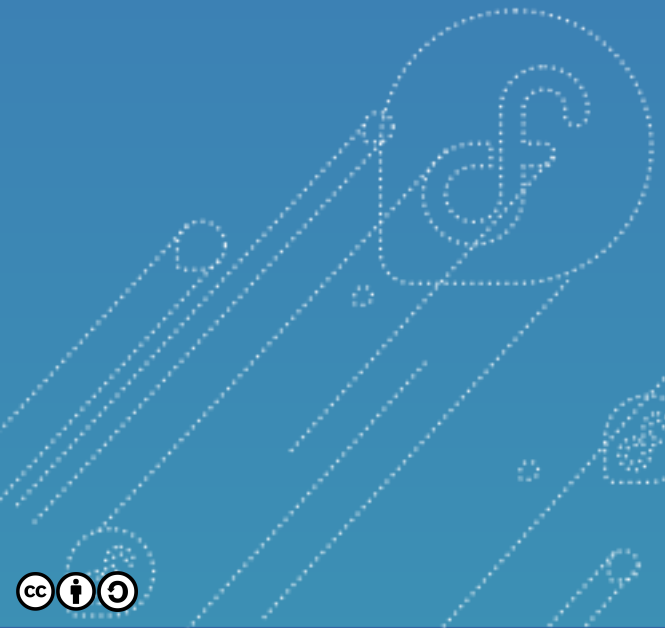
- About myself: I love to listen to other people's stories, learning to play the transverse flute, originally from Brazil but living in Europe for the past 5 years!

Assumed Knowledge

- A basic understanding of cloud computing: cloud providers and VMs
- Basic identity management concepts: hosts and users, SSH, HBAC

But André, I don't know all those things, what about now? Well, there are people in this room more capable than me to answer all your questions, save them for later and we will help you :)

What problem are we trying to solve?



Cloud VMs

So you launched a VM...

- How do you authenticate to it? (most often: SSH keys)
- How does it authenticate to other machines / services?
- What if many users need to access the machine / workload?
- What if someone leaves the company or you have to revoke access?
- How do you enforce access policies?

Identity management approaches for cloud VMs

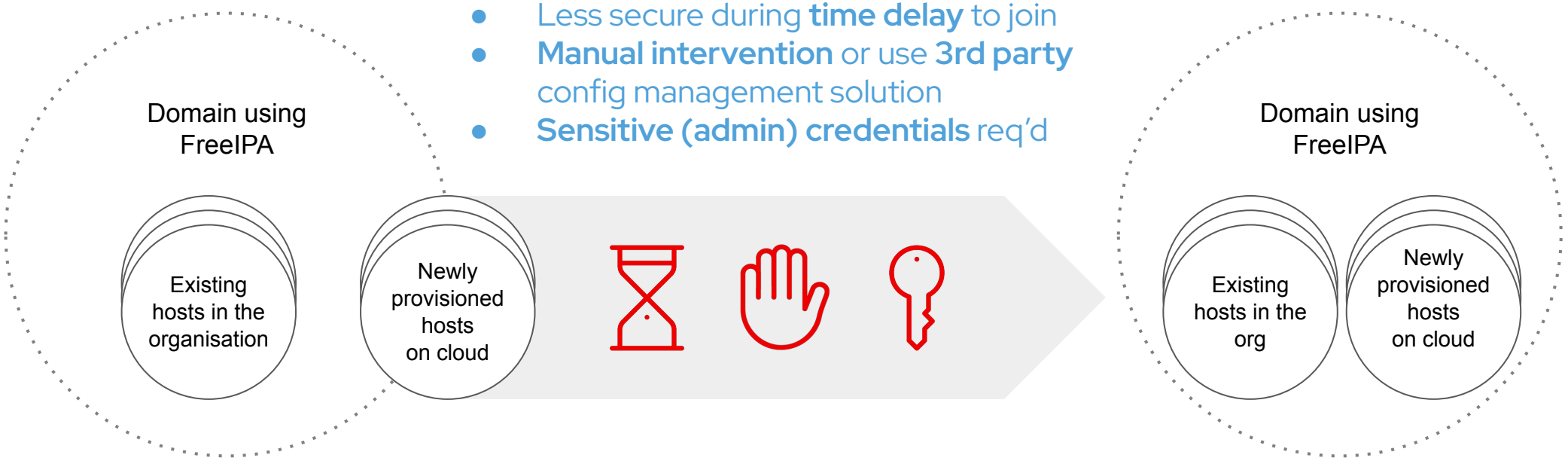
- Just use SSH keys - doesn't scale well
- SSH certificates - scales well, but requires special-purpose PKI
- Privileged Account Management - 3rd party [commercial] solutions
- Corporate IdM (FreeIPA, AD) - need to enrol clients somehow
- Corporate cloud-based IdM (Entra ID) - host authentication techniques not mature

Identity management approaches for cloud VMs

- Just use SSH keys - doesn't scale well
- SSH certificates - scales well, but requires special-purpose PKI
- Privileged Account Management - 3rd party [commercial] solutions
- **Corporate IdM (FreeIPA, AD) - need to enrol clients somehow**
- Corporate cloud-based IdM (Entra ID) - host authentication techniques not mature

Joining cloud VMs - today

- Less secure during **time delay** to join
- **Manual intervention** or use **3rd party** config management solution
- **Sensitive (admin) credentials** req'd



New VMs are not in the IPA domain - no user access except via SSH keys and no policy enforcement

This is the problem

Hosts joined to the domain recognise org users and enforce security policies

The bottom line

- **Reduce complexity and cost** of robust identity management in cloud environments
- Let companies **use their existing IdM** to enable easy and safe transition to hybrid cloud environment
- **Don't sacrifice security** in the name of convenience

Podengo and Red Hat Hybrid Cloud Console

Solution Overview

Podengo Project

- *Portuguese podengo* - a dog with three sub-breeds (a la Kerberos)
- **Pod** (containers) + **Go** (language)
- Every project should have a cute mascot!
- https://github.com/podengo-project

https://commons.wikimedia.org/wiki/File:Podengo_podengo_portobello_sitting.jpg Public domain

Podengo Project

- **idmsvc-backend**: service backend running on Red Hat Hybrid Cloud Console (Golang)
  - OpenAPI spec: github.com/podengo-project/idmsvc-api
- **idmsvc-frontend**: service UI (React / PatternFly / TypeScript)
- **ipa-hcc-server**: *enrollment agent* plugin for IPA server
- **ipa-hcc-client**: client package with auto-join behaviour

Red Hat Hybrid Cloud Console

- Hosted services to manage Red Hat environments
- For **RHEL**: Red Hat Insights, inventory, images, ***Domain Join***
- Supports multiple cloud providers

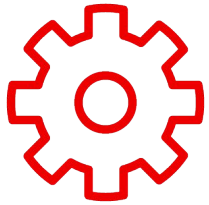
A solution in three acts

1. **Register** your [Free]IPA deployment with Podengo Service (HCC in our case)
2. **Build images** containing the client RPMs
3. **Launch**ed VMs get introduced to IPA, and securely enrol

Domain Join - benefits

Leverage existing IAM

Join cloud VMs to the organisation's existing identity management system



Automatic and immediate

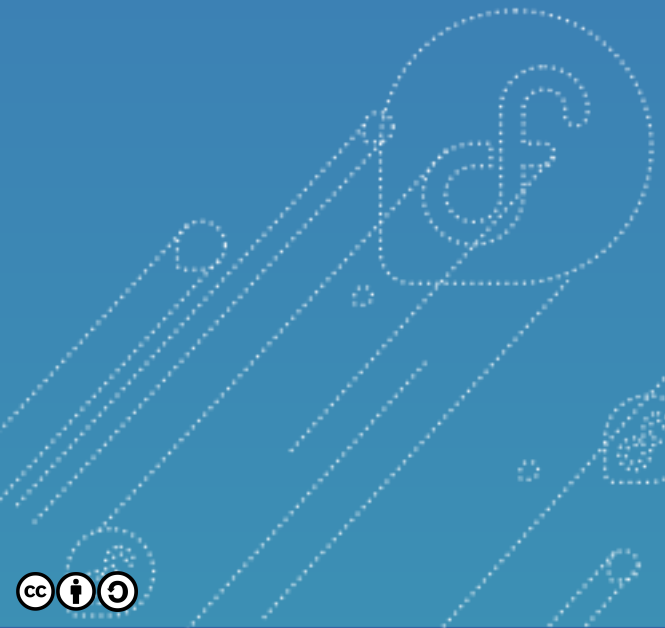
Newly provisioned hosts in their cloud **immediately* join their domain** without any further user intervention.

***less than 2 minutes**

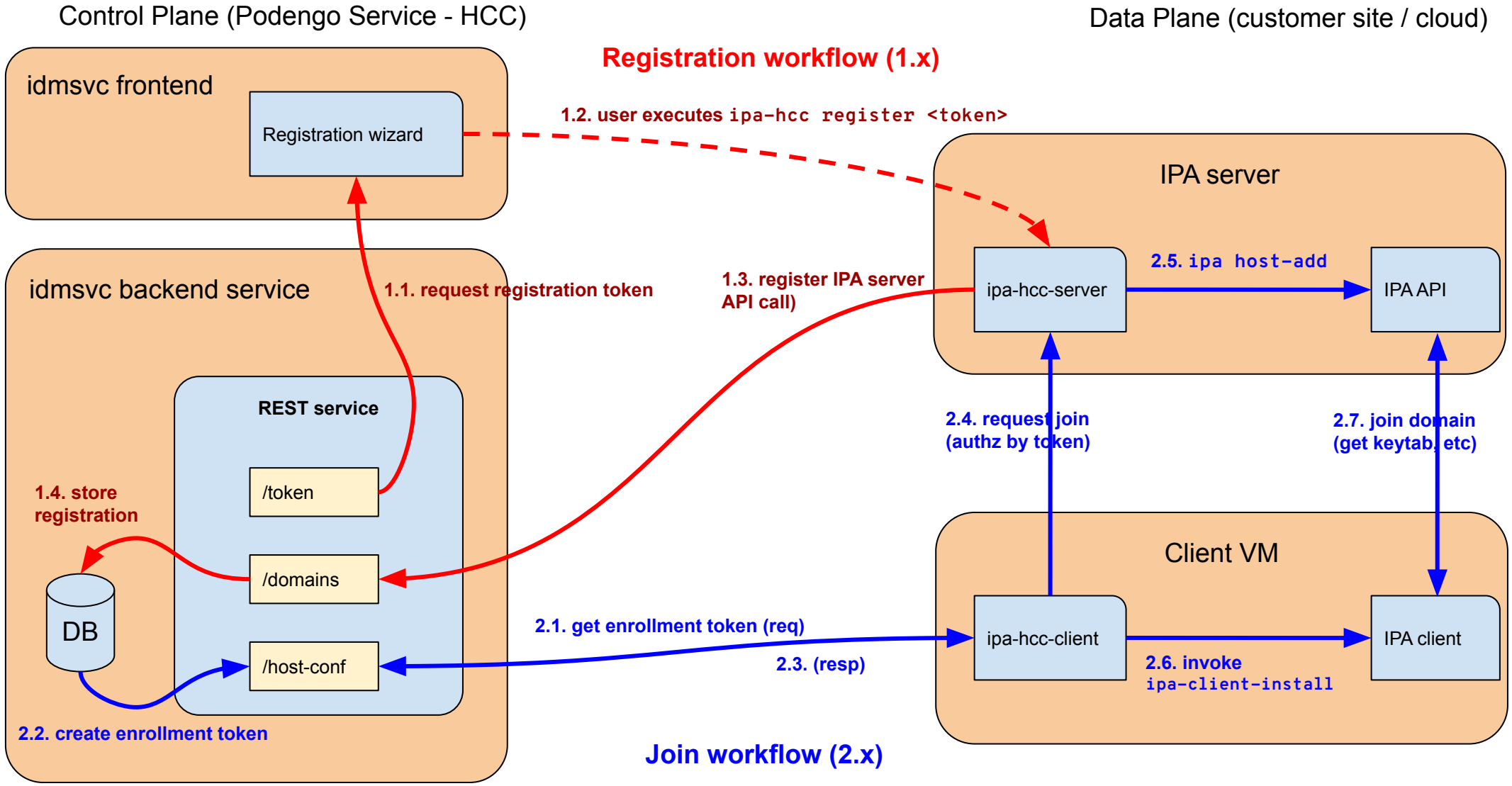
No credentials seen by the service (in this case, HCC)

Launched VMs communicate securely with HCC and the IPA server.

How does it work?



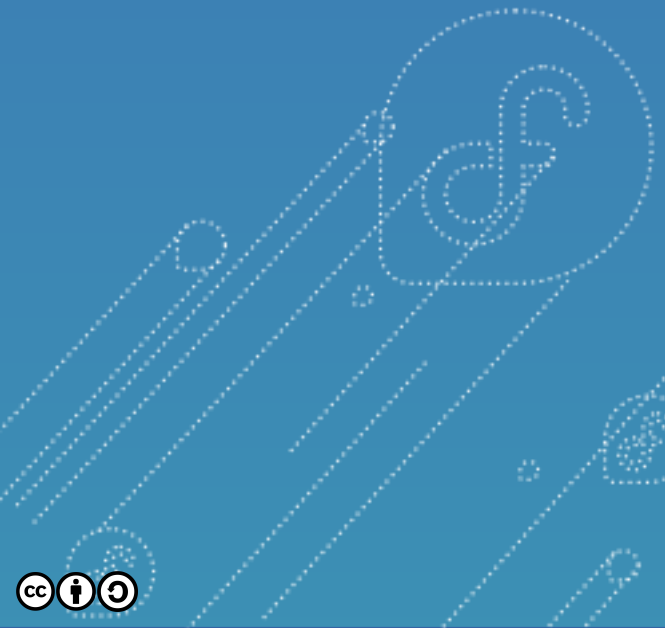
Architecture Overview



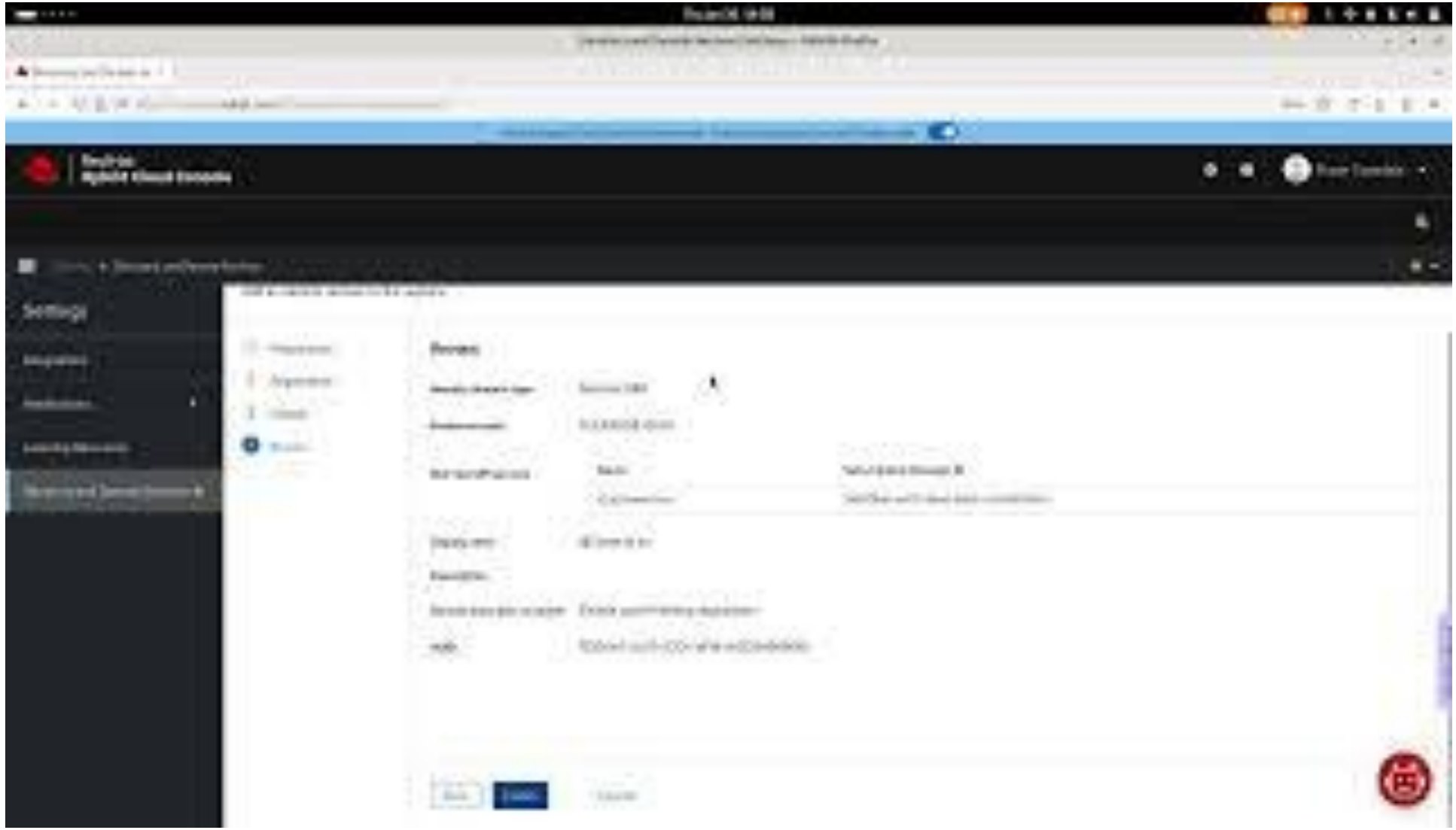
Troubleshooting

- Several things have to be "just right" for this to work
- HCC and IPA server must be reachable from the cloud environment
- DNS, routes and firewalls can all cause problems
- IPA uses lots of ports for lots of protocols: https, ldap, ldaps, kerberos, kpasswd, dns, ...
- Clocks have to be in sync
- **tl;dr** *it's always DNS*

Demo

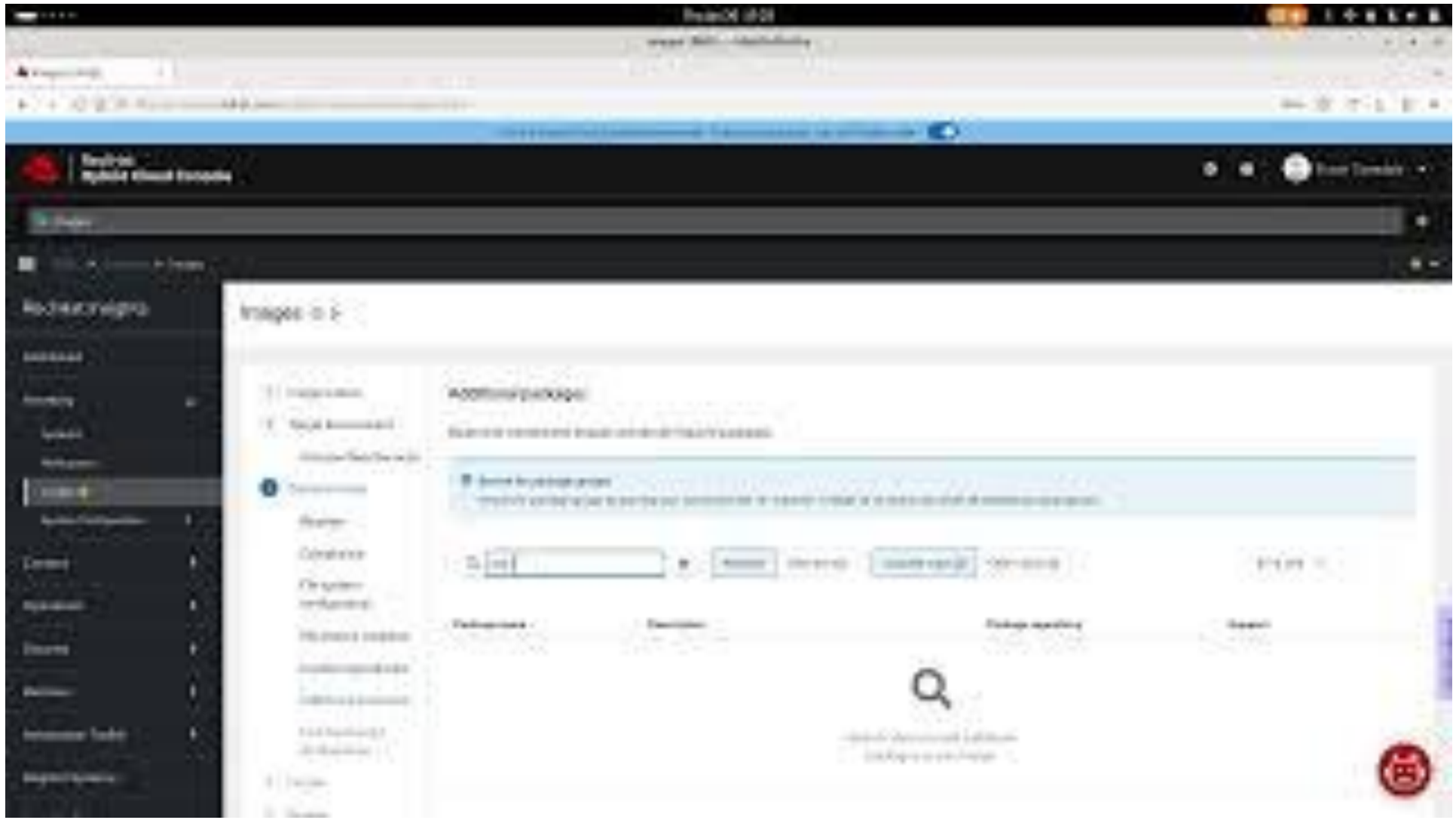


Step 1: Registration



https://is.gd/MMhFHE

Step 2: Building an image

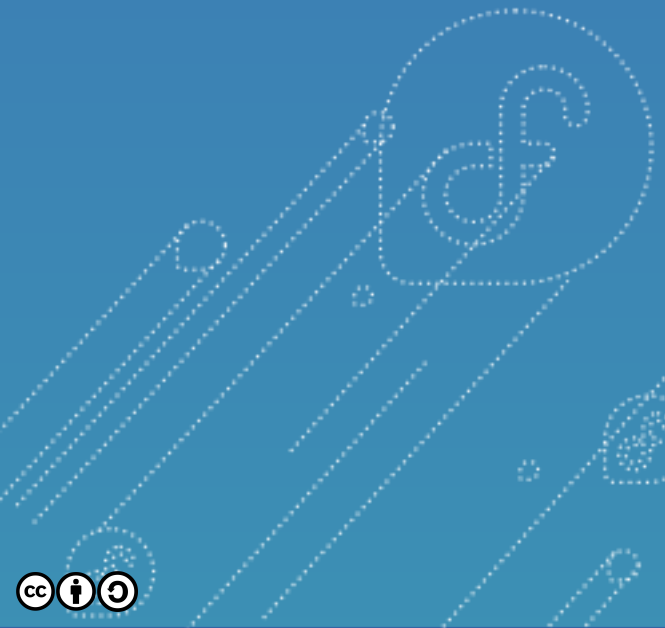


https://is.gd/DWerVj

Step 3: Launch and Connect

https://is.gd/DTtFvG

Status, gaps, and possible futures



Current status

- Feature is **in production** on Hybrid Cloud Console - **preview mode**
- ipa-hcc-{server,client} RPMs are in **Fedora and EPEL** (RHEL later)
- **Documentation** is published but needs expansion
- Cloud provider-specific **onboarding guides** to come
- Collecting metrics and user / customer feedback to inform next steps
- Feedback from **community is more than welcome!**
- Limitation: **one active domain** per org

What could come next?

- Add **Active Directory support**
  - Expand solution to **more organisations**
- Verify / assist users with cloud environment set up
  - **Improve user success** without expanding scope
- Support for multiple domains
- Other HCC-specific integrations

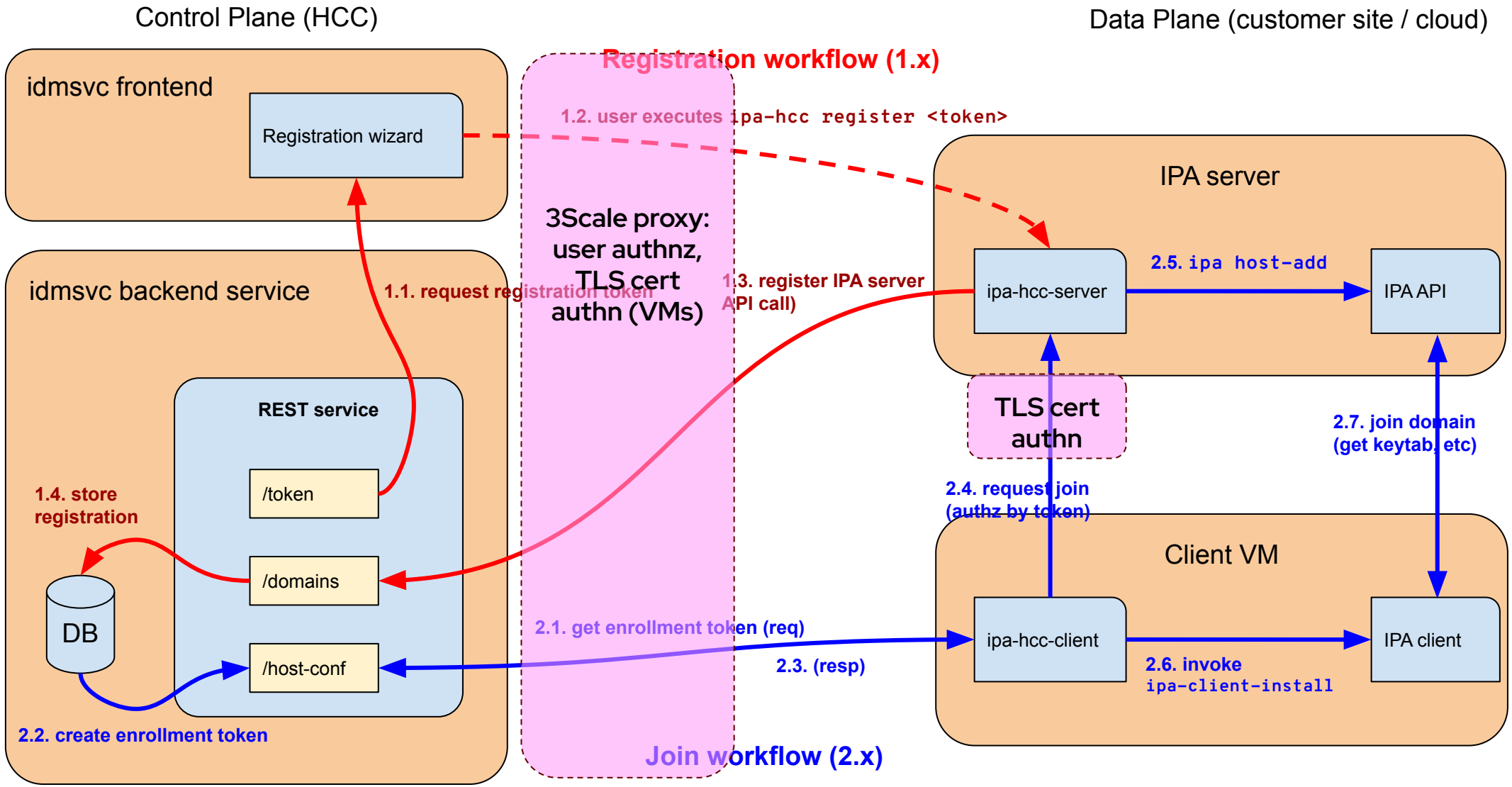
A grand vision

- Hosts consume `console.redhat.com` user identities
- Single unified identity domain
- Option 1: **IPA with External IdP** (requires IPA)
  - Don't miss Sumit's talk at **12:35!**
- Option 2: **localkdc** (no IPA, hosted IdP -> reduced effort and cost)
  - Enable POSIX system login from cloud / web SSO
  - Don't miss Alexander & Andreas' talk at **13:35!**

Non-Insights/HCC applications

- Our architecture** is **not tightly bound to HCC**
  - **shameful truth: the code kinda is...
  - HCC: hosts the idmsvc, **authenticates clients**
- What is required to **use Podengo in other contexts?**
  - X.509 certs for backend/IPA/PKINIT authentication
  - **OR** some other way to authenticate VMs + extend VM->IPA protocol to enable **OTP join**
- Got a use case? Please tell us about it! (GitHub issue, mailing list)

Architecture Overview



Conclusion

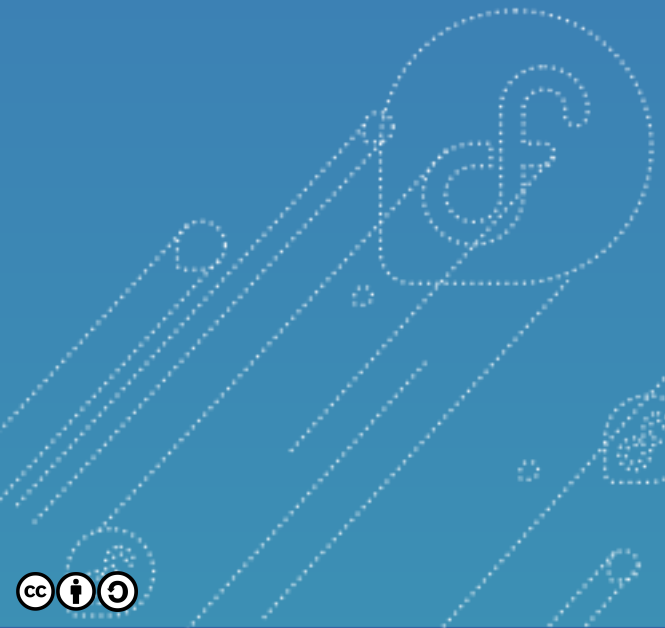
Resources

- Official docs: Deploying and managing RHEL systems in hybrid clouds | Red Hat Product Documentation
- github.com/podengo-project
- EO2024 talk: Passwordless Linux FreeIPA - Passkey and External IdP login with FreeIPA
- EO2023 talk: Kerberos PKINIT (video ; slides)
- Mailing list: freeipa-users@lists.fedorahosted.org
- This slide deck: https://is.gd/DJzCFF
- Linkedin: https://www.linkedin.com/in/andreboscatto/

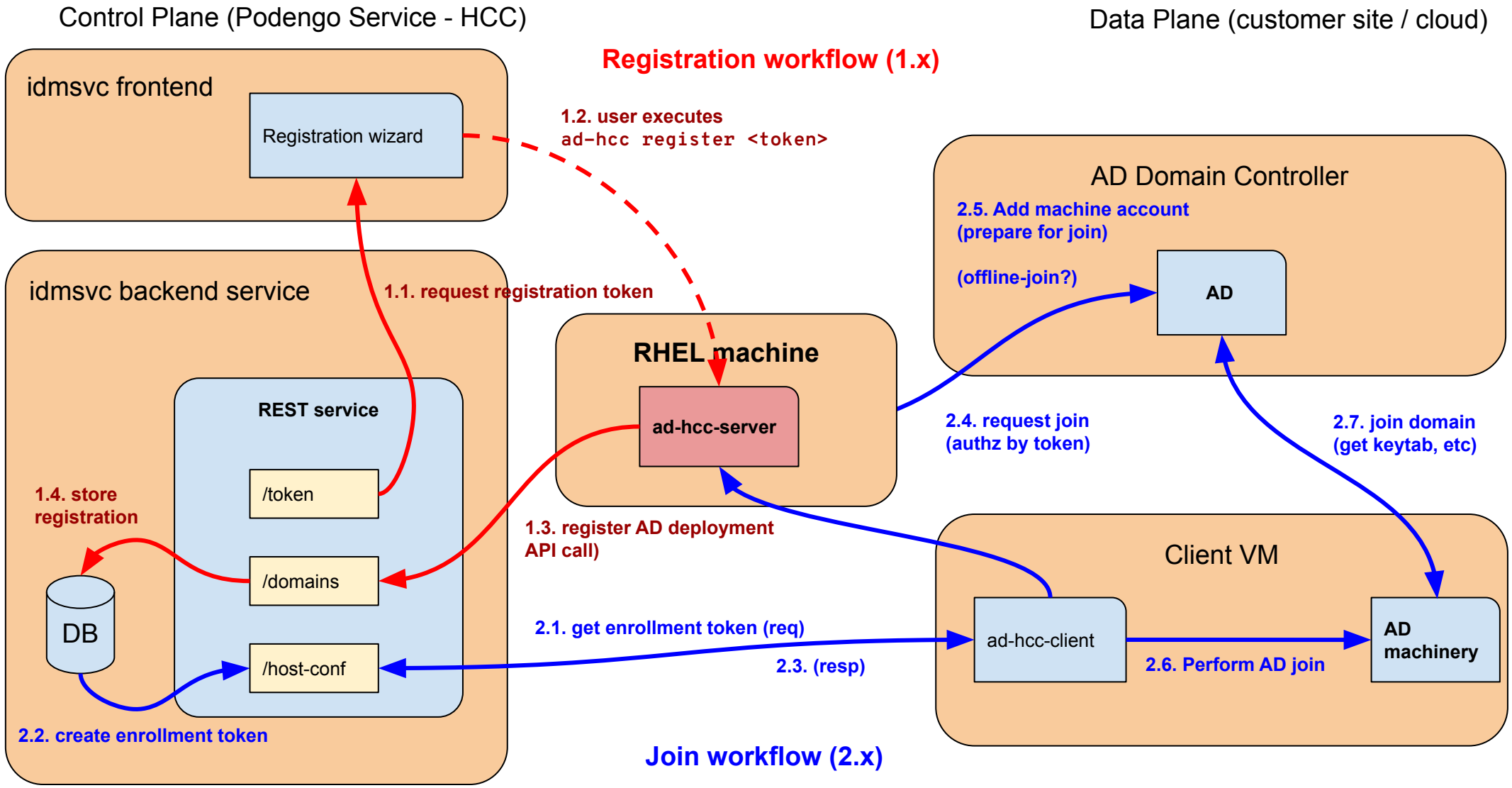
Questions?

https://commons.wikimedia.org/wiki/File:Three_Weavers_Cloud_City_Hazy_IPA.jpg

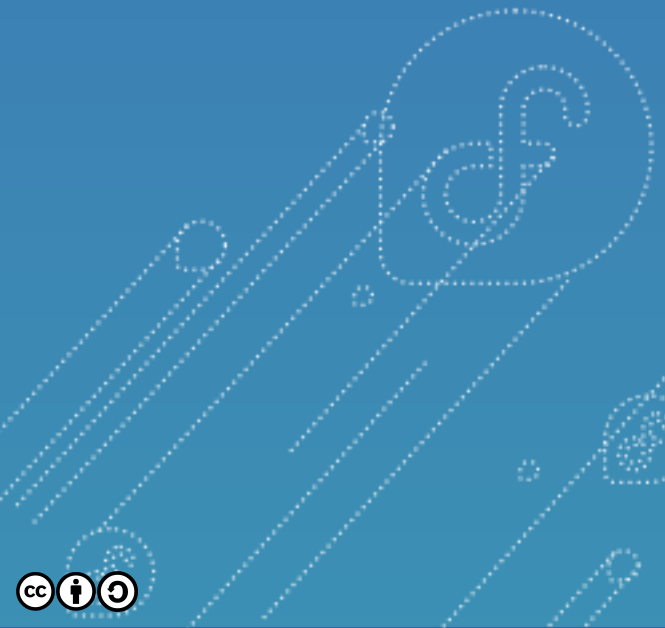
Bonus content unlocked!



Architecture Overview (AD)



FAQ



Why does it take 2 minutes to enroll the machine?

- In the infrastructure Podengo Service is installed, a lot of processes are involved, such as Red Hat Subscription manager, insights, etc. In a different infrastructure, you might be able to speed up things.

Do I have to install hcc-server on all my servers?

- No, you can install it on one or two machines.

- Running the command *ipa-hcc register* once takes care of the whole deployment (server-wise)

My topology changed, what does it happen?

- Podengo ha a job service to take care of that. Or you can run it manually in case you want.

What happens if we remove a VM? Does it get unrolled?

- We are glad you asked! Currently we do nothing, we didn’t find an easy way to detect if a machine went away and the host entry has to be removed.

- If you have a good idea about how to tackle it down, we would love to hear!